power SPEED privat
das Glasfasernetz der Energie AG

Benutzerhandbuch

PM520 LWL Router

ENERGIE AG Data
Wir denken an morgen

Inhaltsverzeichnis

Inhaltsverzeichnis 2
Über das Handbuch 3
Einleitung 3
Vorsichtsmaßnahmen 4
Energie AG – FTTH Kundengerät 5
PM520 Vorderseite 5
PM520 Rückseite 6
Einrichten der Anschlüsse 7
Wandmontage des Gerätes 7
Ethernet-Eigenschaften 8
VoIP-Eigenschaften 8
WLAN Eigenschaften 9
Allgemeines 9
Login am Heimrouter 10
LAN IPv4 DHCP Einstellungen 11
Wireless Einstellungen (WLAN) 12
Wireless Sicherheitseinstellungen 13
Advanced Wireless Einstellungen 14
User Management 15
URL Filter 16
Firewall 17
MAC Filter 18
Security Filter 19
UPnP 20
NAT ALG Settings 21
NAT DMZ Settings 22
NAT Virtual Server Settings 23

Über das Handbuch

Dieses Handbuch beschreibt, wie das FTTH Kundenendgerät PM520 installiert und konfiguriert wird. Das Handbuch richtet sich speziell an Personen, die über Grundkenntnisse im Netzwerkbereich verfügen.

> ☛ **Bitte beachten Sie, dass nicht alle Einstellungen geändert werden können.**

Einleitung

Die neueste Light Link® PM520 Series P2MP ONU ermöglicht eine zukunftsweisende Bandbreite bis 1000 Mbps, maßgeschneidert für FTTH Dienstleistungen. Die kompakte Bauweise berücksichtigt speziell jene Aspekte der Sicherheit und Einfachheit der Installation.

Nachfolgend werden spezielle Aspekte beim Betrieb des LWL Routers herausgegriffen, um so den Benutzer bestmöglich im Betrieb des Routers zu unterstützen und möglichen Fragen vorzubeugen.

Vorsichtsmaßnahmen

ACHTUNG!

Das Gerät ist für die Anwendung im Innenbereich ausgerichtet. Um Feuer, Stromschlag oder eine Beschädigung des Gerätes zu vermeiden, darf das Gerät weder Wasser noch Feuchtigkeit ausgesetzt werden.

- Es muss für ausreichende Kühlung und Lüftung, wie angegeben, gesorgt werden.
- Die Bedienungsanleitung des Produktes muss gelesen und verstanden werden, bevor das Gerät in Betrieb genommen wird.
- Setzen Sie stets die Schutzkappen wieder auf die optischen Anschlüsse, wenn sie nicht verwendet werden.
- Der typische Anschluss ist SC/APC 8 °.
  Hinweis: Ein 8° Grad polierter Stecker muss verwendet werden.
- Gefährliche Spannungen sind innerhalb des Netzteils immer vorhanden.
- Das Gerät darf nicht betrieben werden, sofern nicht alle Abdeckungen und Panels ordnungsgemäß installiert wurden.

Reinigung

Für die Reinigung der Vorderseite verwenden Sie lediglich ein feuchtes Tuch. Verwenden Sie ein weiches, trockenes Tuch, um die Oberseite des Gerätes zu reinigen. Verwenden Sie keine Reinigungssprays jeglicher Art.

Überlastung

Eine Überlastung der Steckdosen und Verlängerungskabel erhöht die Gefahr von Bränden oder elektrischen Schlägen. Verwenden Sie das empfohlene Netzteil mit dem richtigen Kabel und dem richtigen Stecker für den Einsatz des Gerätes.

Schäden mit Reparaturbedarf

Trennen Sie das Gerät und lassen Sie dieses nur von dafür qualifiziertem Servicepersonal von Pacific Broadband Networks warten bzw. reparieren. Versuchen Sie nicht, dieses Gerät selber zu warten.

ACHTUNG!

Eine Gefährdung durch Laserstrahlung der Klasse 1M ist möglich. Zugang sollte nur einem beschränkten und entsprechend geschulten Personal gewährt werden. Freiliegende Fasern oder aber auch Stecker sollen beim Umgang mit optischen Geräten nicht näher inspiziert werden.

Energie AG – FTTH Kundengerät

PM520 Vorderseite

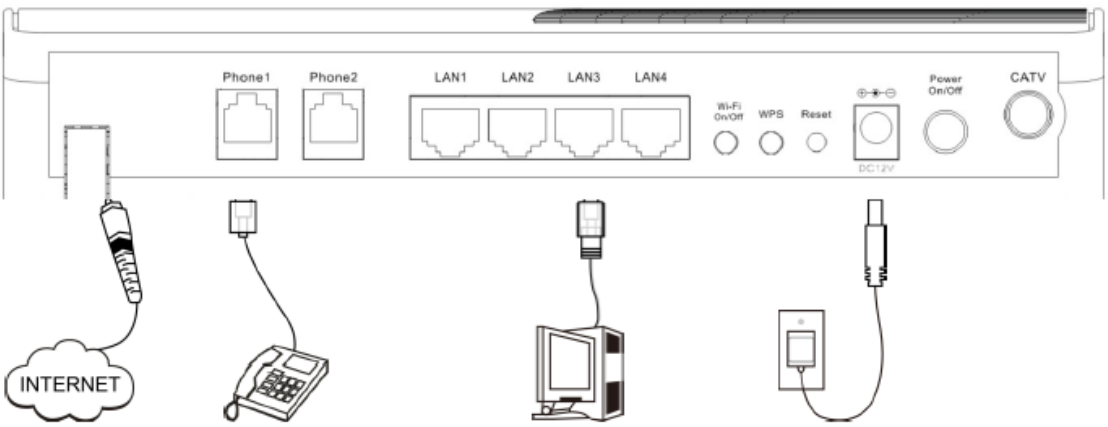
LED	Funktion	
WPS	AUS	WLAN Protected Setup nicht aktiv
	Blinken	WLAN Protected Setup läuft
Wi-Fi	AUS	WLAN aktiv
	EIN	WLAN ist konfiguriert und aktiv
	Blinken	WLAN entdeckt
Power	AUS	Keine Stromversorgung des Gerätes
	EIN	Stromversorgung des Gerätes funktioniert korrekt
Fiber Link	AUS	Router ist nicht an der Zentrale registriert.
	EIN	Router ist an der Zentrale registriert.
	Blinken	Router wurde nicht korrekt bei der Zentrale registriert
Alarm	AUS	Kein Alarm
	Rot	Keine Glasfaserverbindung hergestellt
LAN 1-4	AUS	Keine Ethernet-Verbindung hergestellt.
	EIN	Grün = 1000 Mbps, Orange = 100 Mbps, Gelb = 10 Mbps
	Blinken	Die Datenübertragung läuft (bei jeder Geschwindigkeit).
Phone 2	AUS	Phone 2 ist nicht beim SIP Server registriert.
	EIN	Phone 2 ist beim SIP Server registriert.
	Blinken	Phone 2 ist derzeit abgehoben oder in Verwendung.
Phone 1	AUS	Phone 1 ist nicht beim SIP Server registriert.
	EIN	Phone 1 ist beim SIP Server registriert.
	Blinken	Phone 1 ist derzeit abgehoben oder in Verwendung.
System	Blinken	System wird gestartet
	AUS	System bereit

	Blinken	System funktioniert nicht

PM520 Rückseite

Element	Beschreibung
Phone 1	Telefon 1 – RJ11 Anschluss
Phone 2	Telefon 2 – RJ11 Anschluss
LAN 1-4	Gigabit Ethernet Ports, 4xRJ45 – 10/100/1000 Mbps
WPS Button	Drücken und halten Sie die WLAN-Taste für 3 Sekunden, um das WLAN zu aktivieren / deaktivieren
Reset Button	Reset-Taste, um die Werkseinstellungen wiederherzustellen
DC12V Power Port	Netzbuchse für 11 bis 15V DC Netzteil
Power On/Off	An-/Aus-Schalter für PM520

Einrichten der Anschlüsse



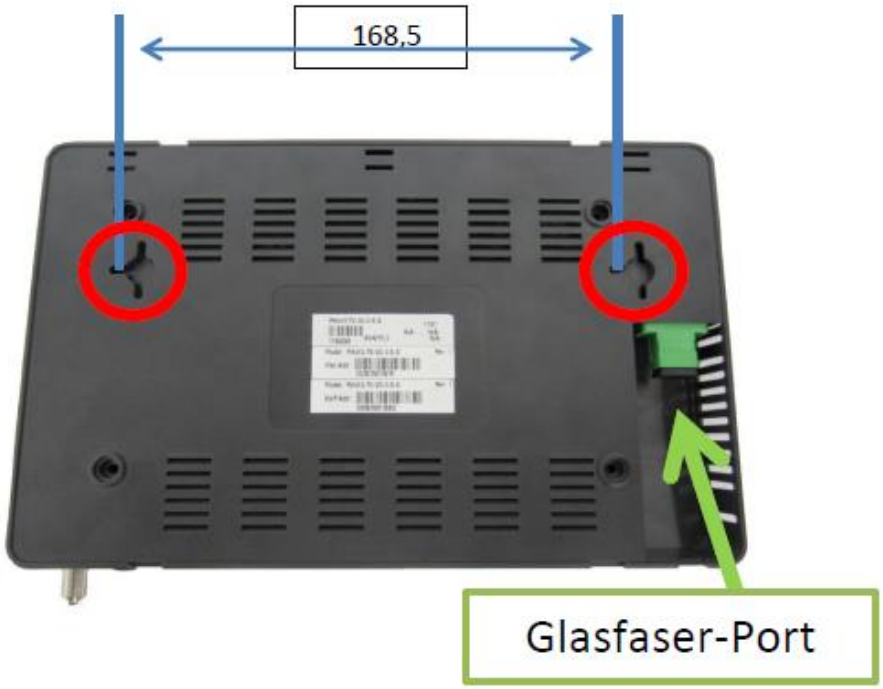
Schließen Sie ihr Gerät gemäß folgenden Schritten an, um Ihr Glasfasernetz zu nutzen:

1. Verbinden Sie den „PON Port" mit dem Lichtwellenleiter-Anschluss vom Typ SC
2. Verbinden Sie das Telefon mit dem „FXS Port" mittels RJ-11 Telefonanschlusskabel.
3. Verbinden Sie den PC mit dem Ethernet Port mittels RJ-45 Cat5/Cat6 Kabel
4. Verbinden Sie den Gerätenetzanschluss mittels des Netzteils. Drücken sie den Knopf „Power On/Off" um das Gerät zu starten.

Wandmontage des Gerätes

Sie können das Gerät auf einer senkrechten Fläche mit Hilfe der vorgeformten Montagelöcher auf der Unterseite des Gerätes und den zwei Plattenkopf-Holzschrauben befestigen.

- Befestigen Sie die Schrauben in der Wand. Die Position der Schrauben muss in der gleichen horizontalen Linie sein und den gleichen Mittenabstand wie die Befestigungslöcher haben. Lassen Sie die Schraubenköpfe mindestens 6 mm aus der Wand herausstehen. Hängen Sie das Gerät durch die Befestigungslöcher an die Schrauben.



Ethernet-Eigenschaften

Schnittstelle	4x10/100/1000 Mbps auf RJ45, Full/Half-Duplex, Auto-Negotiation, Auto MDI/MDIX
VLAN	IEEE802.1Q, QinQ unterstützt
Spanning Tree Protocol	IEEE802.1D unterstützt, > 64 MAC pro Gerät (RSTP standardmäßig aktiviert)
QoS	IEEE802.1p, DiffServ Unterstützung, 4 Queues pro Port
Framegröße	64 bis 1522 Bytes
IGMP	IGMP (v1, v2) Snooping Support
Security	Broadcast / Multicast Storm Unterdrückung, Accesslisten und -filter

VoIP-Eigenschaften

VoIP	SIPv2
SIP Codecs	G.711,G.723.1,G.726_24, G.726_32,G.729A
Eigenschaften	Anrufweiterleitung Anruf halten/ abgeben Anklopfen Anrufer-ID Echo-Unterdrückung (LEC) Adaptiver Jitter-Puffer Paketverlustsverschleierung Comfort Noise Generator
DHCP	Option 66 & 67, Auto-Provisioning Unterstützung
Telefonanschlüsse	2 x RJ11 (POTS)

WLAN Eigenschaften

Standards	802.11 b/g/n
Konfigurations-optionen	1) 2 x 2 (2.4 GHz) – minimaler Durchsatz 40 Mbps
WLAN-Security	WLAN Verschlüsselung: WPA2-PSK; WPA-PSK; WEP; Open Weitere Security Features: WLAN MAC Adressenfilter
QoS	WMM-QoS (für Multimediaapplikationen)
Setup/ Konfiguration	WPS Unterstützung (WLAN geschütztes Setup) Webkonfiguration
Mehrere SSIDs	Unterstützt bis zu 4 SSIDs Standard SSID ist vorkonfiguriert.
WLAN Kanal Konfiguration	Standard: Automatische Kanalwahl (basierend auf Congestion Scan) Manuelle Auswahl
Konfigurierbare Parameter	DTIM Intervall Fragmentierungsschwelle RTS Schwelle 802.11n-Übertragungsrate CTS Schutzmodus SSID Broadcast aktivieren/ deaktivieren
Antennen	Interne Antenne

Allgemeines

Eingangsspannung	11-15V DCdc
Netzstromgerät	100~240V AC, 50~60 Hz, 0.5 A max.
Leistungsaufnahme	< 8.5 W (Vollbeladen)
Dimension (H x W x D)	46 mm x 207 mm x 147 mm
Nettogewicht	0.55 kg

Login am Heimrouter

Sie können Ihren WLAN Router ganz einfach über die Weboberfläche Ihrer Browsers bedienen und konfigurieren.

Gehen Sie wie folgt vor:

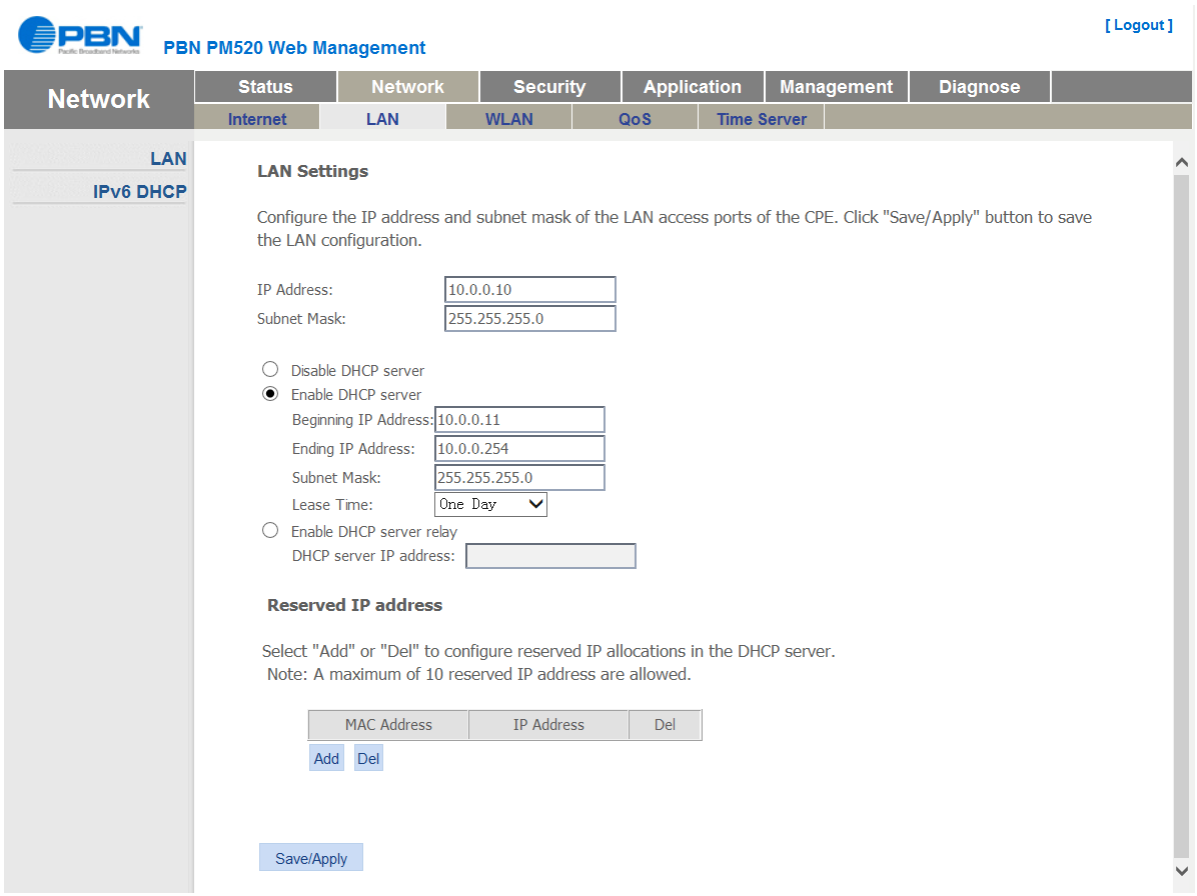
1. Starten Sie ihren Webbrowser (Internet Explorer, Firefox, Chrome, usw.)
2. Geben Sie die IP Adresse des Routers ein: **http://10.0.0.10**
3. Es erscheint ein Anmeldefenster Ihres Routers.
    a. Default-Login: **user / changeme** (Wir weisen darauf hin dieses Passwort umgehend zu ändern)
4. Klicken Sie auf **"Submit"** um in den Konfigurationsmodus zu gelangen.

Sie können diese Einstellungen auch von Ihrem Smartphone, Tablet oder per WLAN verbundenen PC aus konfigurieren. Sie müssen hierzu nur mit Ihrem WLAN-Netz verbunden sein!

LAN IPv4 DHCP Einstellungen

Im Webinterface Ihres Routers, klicken Sie auf " **Network** " in der obersten Reihe, dann auf "**LAN**" und schließlich "**LAN**" auf der linken Seite.

Die LAN-Einstellungen erscheinen.



Auf dieser Seite können Sie folgende Parameter einstellen:

- LAN IP Adresse und Subnet (IP Adresse des Routers = Default Gateway)
- Enable/Disable DHCP Server
- IPv4 Lease-Dauer
- IP/MAC address assignment

Klicken Sie nach dem Ändern auf "**Save/Apply**", um Ihre Einstellungen dauerhaft zu speichern.

Wireless Einstellungen (WLAN)

Auf dem Webinterface des Routers, klicken Sie auf **"Network"** im oberen Reiter, dann den "**WLAN"** Button**,** und dann auf **"WLAN Basic"** auf der linken Seite.

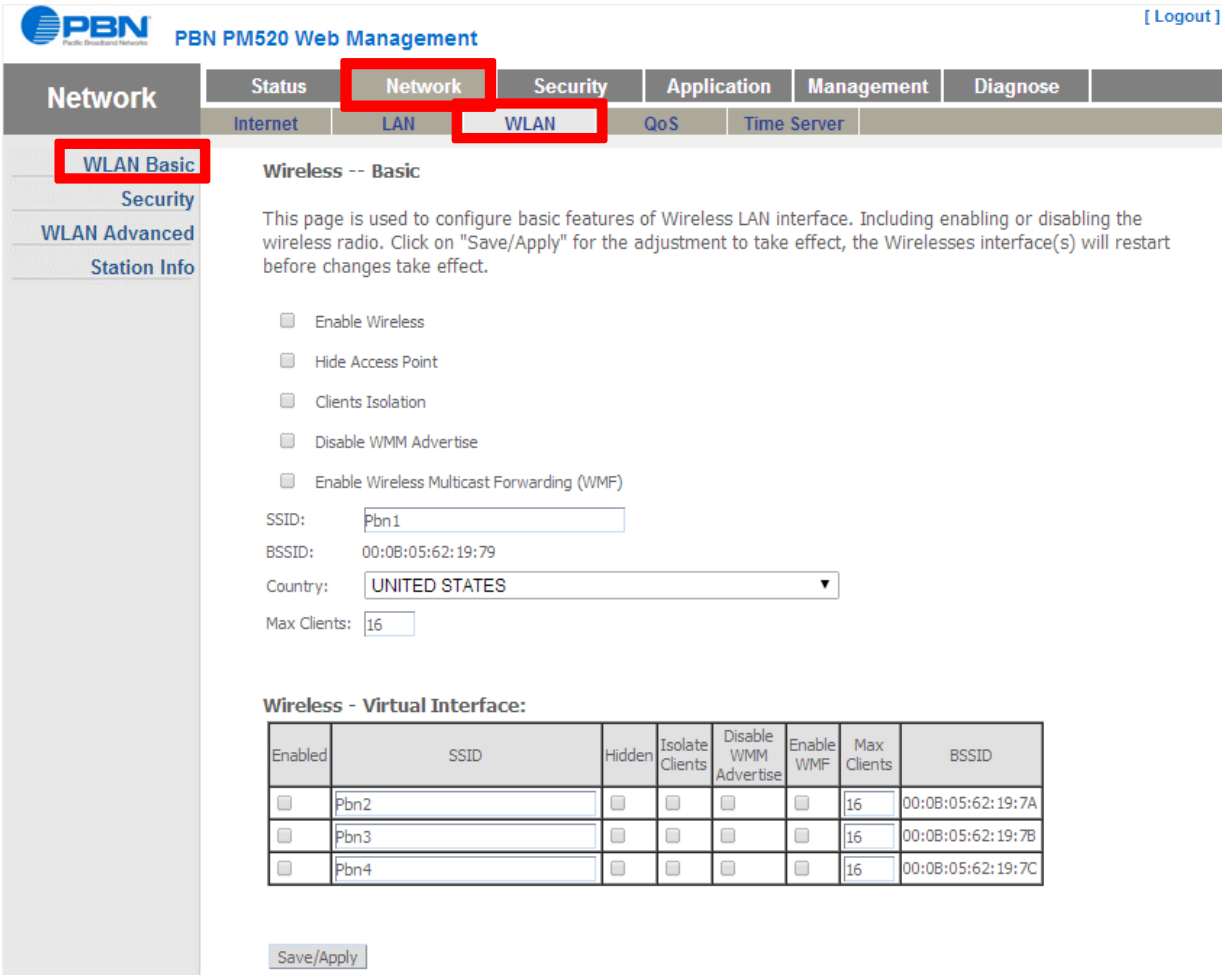
Die Wireless- oder WLAN Einstellungen erscheinen.

Das Wireless-LAN ist bei Auslieferung deaktiviert! Dies können Sie ändern indem Sie **„Enable Wireless"** anhacken und anschließen "**Save/Apply" klicken**

Auf dieser Seite können Sie die Basiseinstellungen Ihres WLAN (WIFI) ändern. Hier haben Sie die Möglichkeit, unter anderem die SSID (WLAN-Name) zu ändern, die Ländereinstellung vorzunehmen, die maximale Teilnehmeranzahl pro SSID einzustellen, das WIFI-Multicast-Forwarding (WMF) zu konfigurieren sowie User-Isolationen durchzuführen.

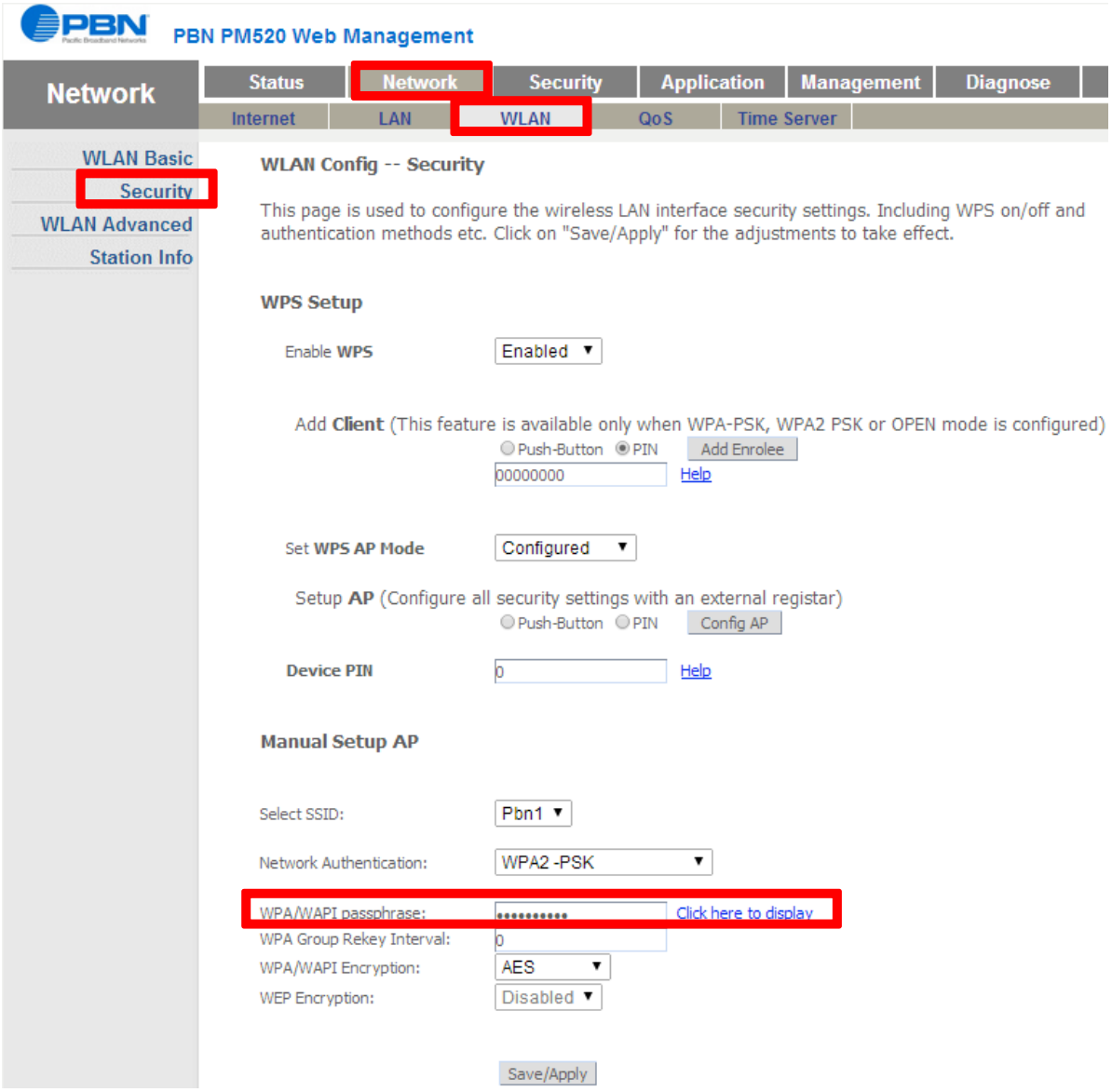
Stellen Sie sicher, dass Ihr WLAN durch Aktivieren des Punktes „Enable Wireless" eingeschaltet und eine SSID (WLAN-Name) eingetragen ist!

Klicken Sie nach dem Ändern auf "**Save/Apply",** um Ihre Einstellungen dauerhaft zu speichern!



Wireless Sicherheitseinstellungen

Auf dem Webinterface des Routers, klicken Sie auf **"Network"** im oberen Reiter, dann den "**WLAN"** Button**,** und dann auf **"Security"** auf der linken Seite.
Auf dieser Seite können Sie die Sicherheitseinstellungen Ihres WLAN (WIFI) einstellen.



In dem "WPS Setup" Bereich können Sie die Wi-Fi Protected Setup (WPS) Funktion einschalten. Durch Drücken der WPS Taste auf der Rückseite des Routers oder durch Eingabe des WPS Codes ihres Endgerätes, können Sie einfach neue Geräte in Ihr Wirelessnetzwerk mitaufnehmen.

Im "Manual Setup AP" Bereich, können Sie die Sicherheitseinstellungen manuell für jede einzelne Ihrer SSID ändern.
Nach dem Auswählen der SSID, die Sie ändern wollen, können Sie die Einstellung für die Art der Verschlüsselung, das Passwort **(WPA/WAPI Passphrase)** sowie die Encryption Methode wählen. Wir empfehlen die Einstellung: WPA2-PSK, AES sowie ein sicheres Passwort.

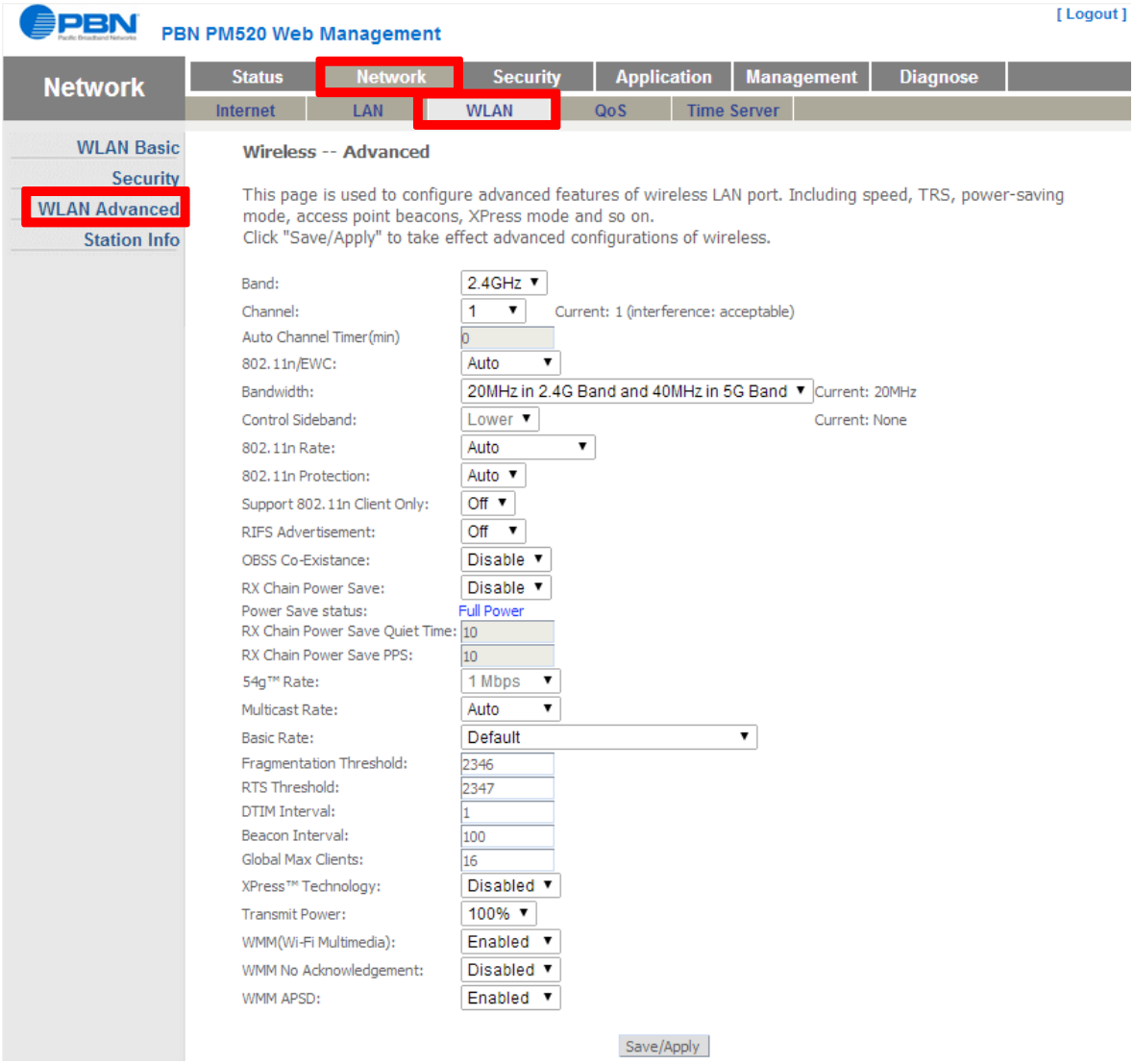
Klicken Sie "**Save/Apply",** um Ihre Einstellungen dauerhaft zu speichern.

Advanced Wireless Einstellungen

Auf dem Webinterface des Routers, klicken Sie auf **"Network"** im oberen Reiter, dann den "**WLAN"** Button**,** und dann auf **"WLAN Advanced"** auf der linken Seite.

Auf dieser Seite können Sie weitere Einstellungen für Ihr Wireless-Netzwerk vornehmen. Wir empfehlen diese Einstellungen nur durch geschultes Personal ändern zu lassen.

Klicken Sie "**Save/Apply"** um Ihre Einstellungen dauerhaft zu speichern.



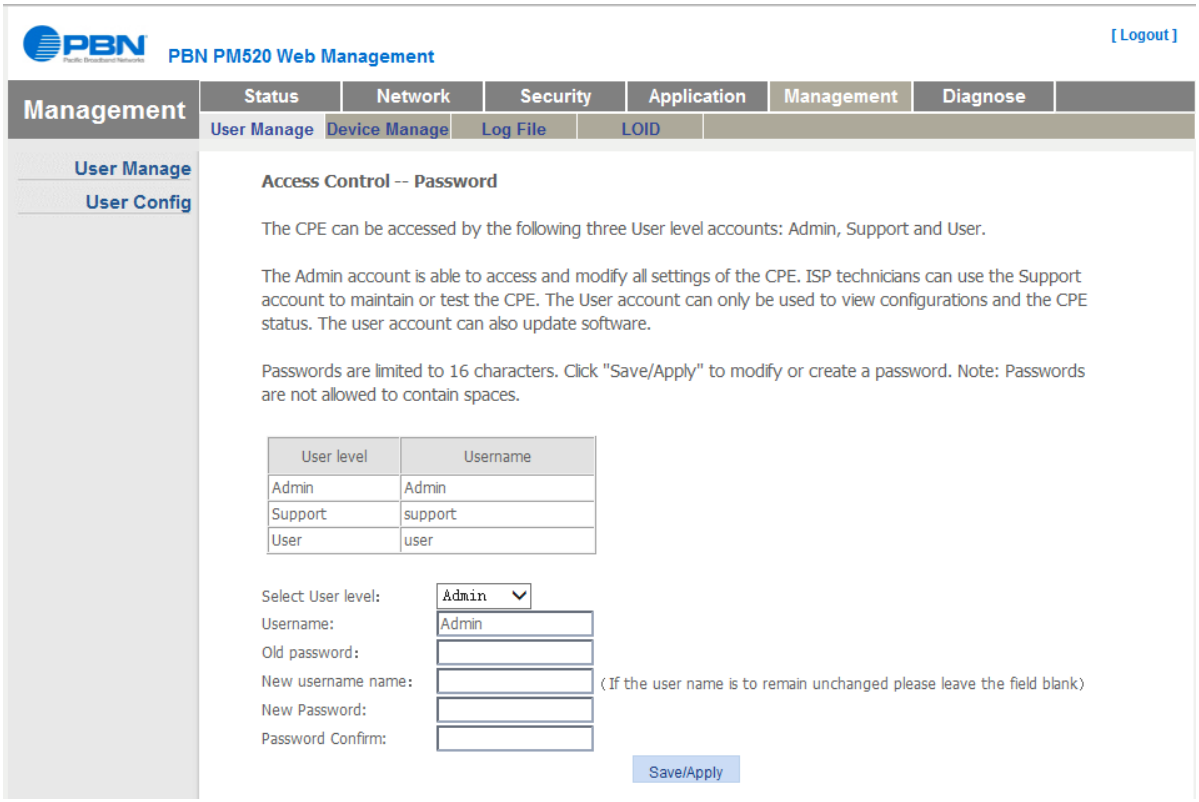
User Management

Auf dem Webinterface des Routers, klicken Sie auf **" Management "** im oberen Reiter, dann den "**User Manage**" Button und dann auf **"User Manage"** auf der linken Seite.

Die User Management Einstellungen erscheinen.

Wir bitten Sie, das Standardpasswört umgehend zu ändern!!!

DER USERNAME SOLL NICHT GEÄNDERT WERDEN! Dieser wird bei Änderung nicht gespeichert!

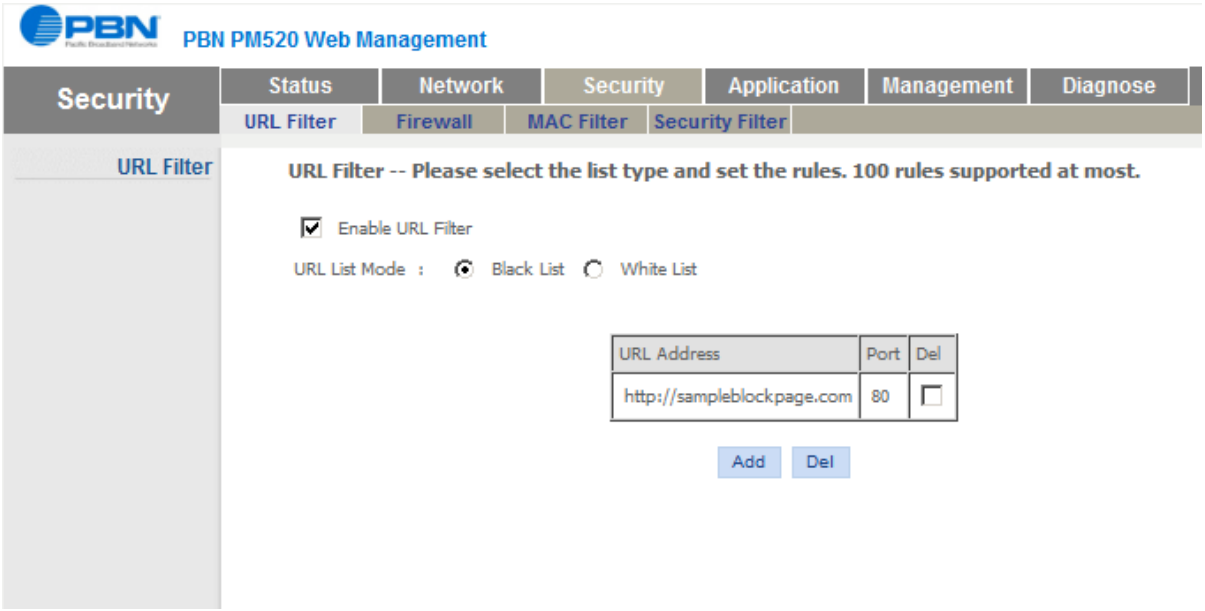

PBN PM520 Web Management
[Logout]
Management
Status
Network
Security
Application
Management
Diagnose
User Manage
Device Manage
Log File
LOID
User Manage
User Config
Access Control -- Password
The CPE can be accessed by the following three User level accounts: Admin, Support and User.
The Admin account is able to access and modify all settings of the CPE. ISP technicians can use the Support account to maintain or test the CPE. The User account can only be used to view configurations and the CPE status. The user account can also update software.
Passwords are limited to 16 characters. Click "Save/Apply" to modify or create a password. Note: Passwords are not allowed to contain spaces.
User level
Username
Admin
Admin
Support
support
User
user
Select User level:
Admin
Username:
Admin
Old password:
New username name:
(If the user name is to remain unchanged please leave the field blank)
New Password:
Password Confirm:
Save/Apply

Sie können auf dieser Seite den USERNAMEN sowie das PASSWORT ihres Routers ändern.
Default User: **user**
Default Passwort: **changeme**
Klicken Sie "**Save/Apply",** um Ihre Einstellungen dauerhaft zu speichern.

URL Filter

Im Webinterface Ihres Routers, klicken Sie auf "**Security**" in der obersten Reihe und schließlich auf "**URL Filter**"

Die URL-Filter Einstellungen erscheinen.



Auf dieser Seite können Sie den URL-Filter für Ihr Heimnetzwerk aktivieren bzw. deaktivieren.

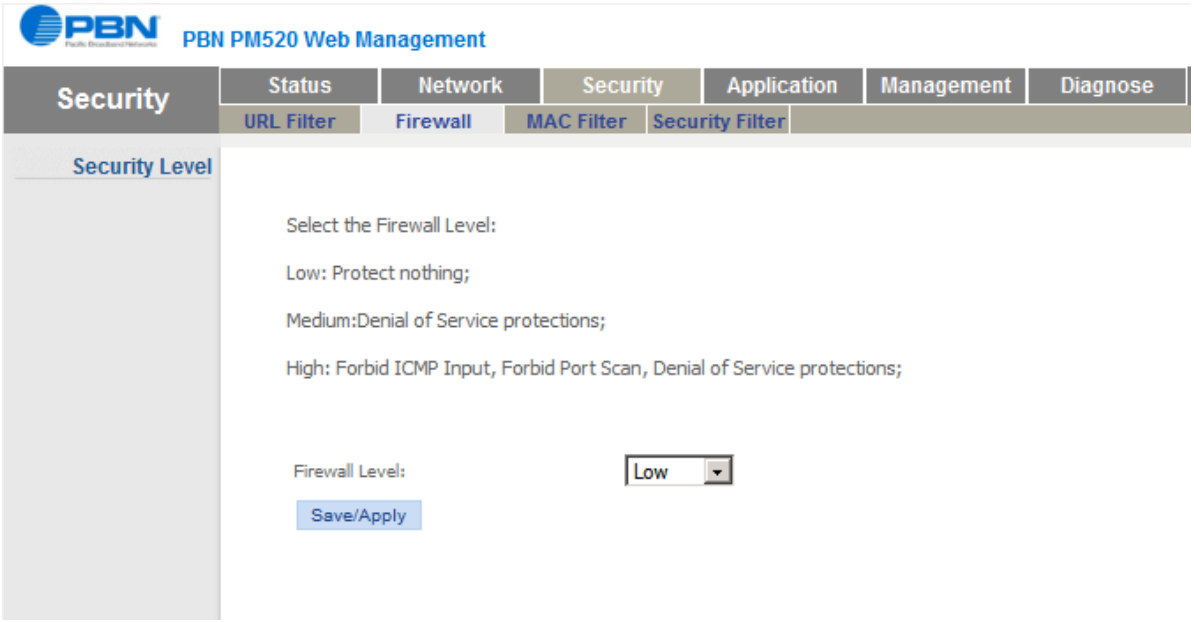
Sie haben 2 Möglichkeiten Webseiten zu sperren:

1. Black List
   a. Mit dieser Einstellung können Sie den **Zugriff auf einzelne Webseiten sperren**.
   b. Klicken Sie auf *„Add"* und geben Sie die Adressen der Webseiten ein (IP-Adresse oder URL), auf die von Ihrem Heimnetzwerk aus nicht zugegriffen werden soll.
   c. Alle anderen Webseiten bleiben von Ihrem Heimnetzwerk **erreichbar.**
2. White List
   a. Mit dieser Einstellung können Sie den Zugriff auf einzelne Webseiten erlauben.
   b. Klicken Sie auf *„Add"* und geben Sie die Adressen der Webseiten ein (IP-Adresse oder URL), auf die von Ihrem Heimnetzwerk aus zugegriffen werden darf.
   c. Alle anderen Webseiten sind von Ihrem Heimnetzwerk **gesperrt.**

Firewall

Im Webinterface Ihres Routers, klicken Sie auf "**Security**" in der obersten Reihe und schließlich auf "**Firewall**"

Die Firewall-Einstellungen erscheinen.



Sie können aus 3 vordefinierten Sicherheitslevel wählen:

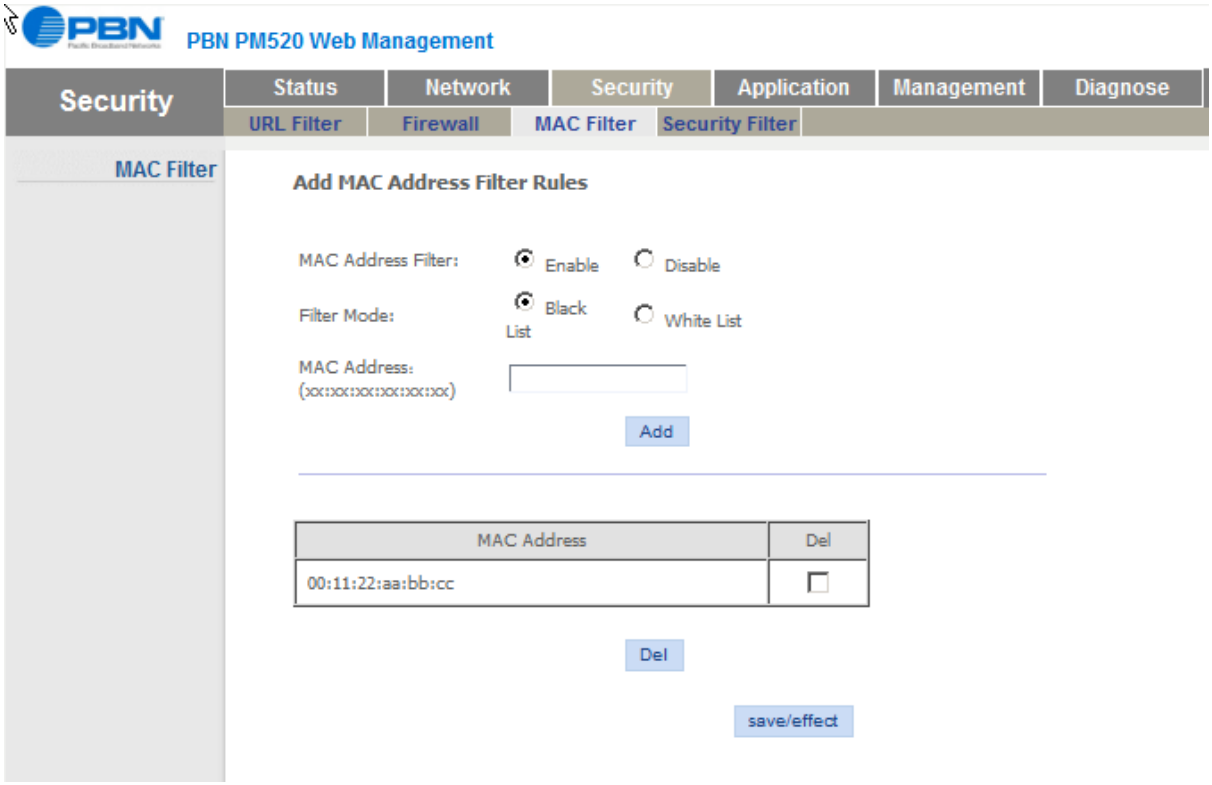
Sicherheitslevel	WAN (eingehende Pakete aus dem Internet)	LAN (ausgehende Pakete aus dem LAN)
Low	Keine Sicherheitseinstellungen; sämtliche Verbindungen aus dem Internet sind erlaubt!	Unbeschränkter Zugriff von Ihrem Heimnetzwerk ins World Wide Web
Medium	Schutz vor „Denial of Service" Attacken; Ausnahmen können in den Port-Forwarding und DMZ Einstellungen vorgenommen werden!	Unbeschränkter Zugriff von Ihrem Heimnetzwerk ins World Wide Web
High	Sämtiche Ports sind von außen gesperrt! Schutz vor „Denial of Service" und „ICMP"-Attacken; Ausnahmen können in den Port-Forwarding und DMZ Einstellungen vorgenommen werden!	Unbeschränkter Zugriff von Ihrem Heimnetzwerk ins World Wide Web

Klicken Sie nach dem Ändern auf "**Save/Apply",** um Ihre Einstellungen dauerhaft zu speichern.

MAC Filter

Im Webinterface Ihres Routers, klicken Sie auf "**Security**" in der obersten Reihe und schließlich auf "**MAC Filter**"

Die MAC Filter Einstellungen erscheinen.



Auf dieser Seite können Sie folgende Einstellungen vornehmen:

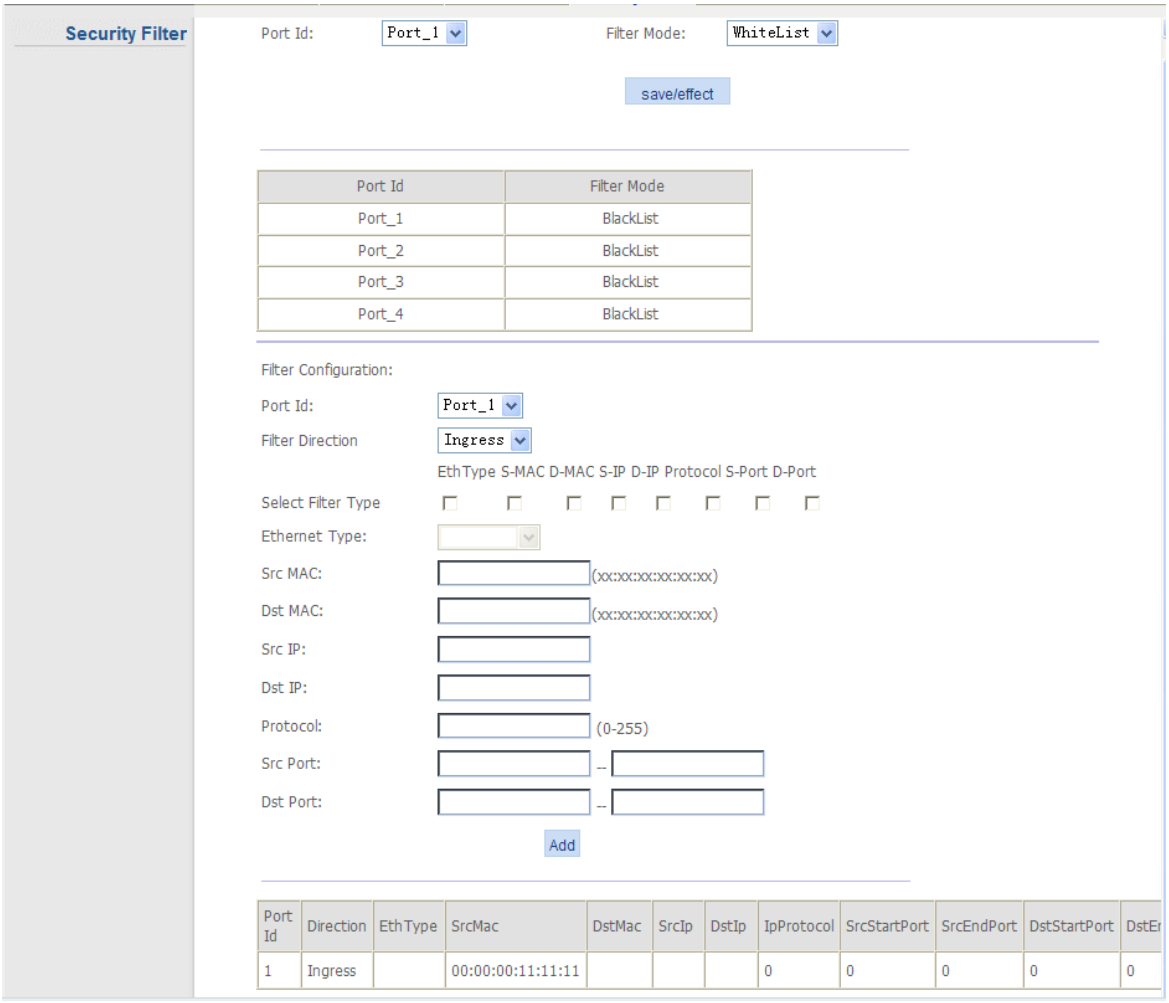
- Enable/Disable MAC Address Filter
- Filter-Modus per Black- oder White List
- MAC Adressen für Filtereinstellungen

Klicken Sie nach dem Ändern auf "**Save/Apply",** um Ihre Einstellungen dauerhaft zu speichern.

Security Filter

Im Webinterface Ihres Routers, klicken Sie auf "**Security**" in der obersten Reihe und schließlich auf "**Security Filter**".

Die Security Filter Einstellungen erscheinen.


Security Filter
Port Id: Port_1
Filter Mode: WhiteList
save/effect
Port Id | Filter Mode
Port_1 | BlackList
Port_2 | BlackList
Port_3 | BlackList
Port_4 | BlackList
Filter Configuration:
Port Id: Port_1
Filter Direction Ingress
EthType S-MAC D-MAC S-IP D-IP Protocol S-Port D-Port
Select Filter Type
Ethernet Type:
Src MAC: (xx:xx:xx:xx:xx:xx)
Dst MAC: (xx:xx:xx:xx:xx:xx)
Src IP:
Dst IP:
Protocol: (0-255)
Src Port:
Dst Port:
Add
Port Id | Direction | EthType | SrcMac | DstMac | SrcIp | DstIp | IpProtocol | SrcStartPort | SrcEndPort | DstStartPort | DstEr
1 | Ingress | | 00:00:00:11:11:11 | | | | 0 | 0 | 0 | 0 | 0

Auf dieser Seite können Sie folgende Einstellungen vornehmen:

- Port ID
- Filter mode
- Filterkonfiguration

Sie können mit diesen Einstellungen den Datenverkehr einzelner LAN-Ports einschränken und steuern. Wir bitten diese Einstellungen nur dann vorzunehmen, wenn Sie einzelne LAN-Segmente voneinander trennen wollen!

Nach dem Auswählen des White/Black-List Modus, können Sie die einzelnen Regeln konfigurieren. Folgende Filterkriterien stehen zur Auswahl: Ethernet-Type, Source-MAC, Destination-MAC, Source-IP, Destination-IP, Protokoll sowie Source- und Destination-Port!

Klicken Sie nach dem Ändern auf "**Save/Apply",** um Ihre Einstellungen dauerhaft zu speichern.

UPnP

Auf dem Web-Interface klicken Sie auf "**Application**" und dann auf den "**UPNP**" Reiter.

Die Einstellmöglichkeit für UPNP erscheint.

Der UPNP-Dienst kann entweder ein-/ oder ausgeschaltet werden.

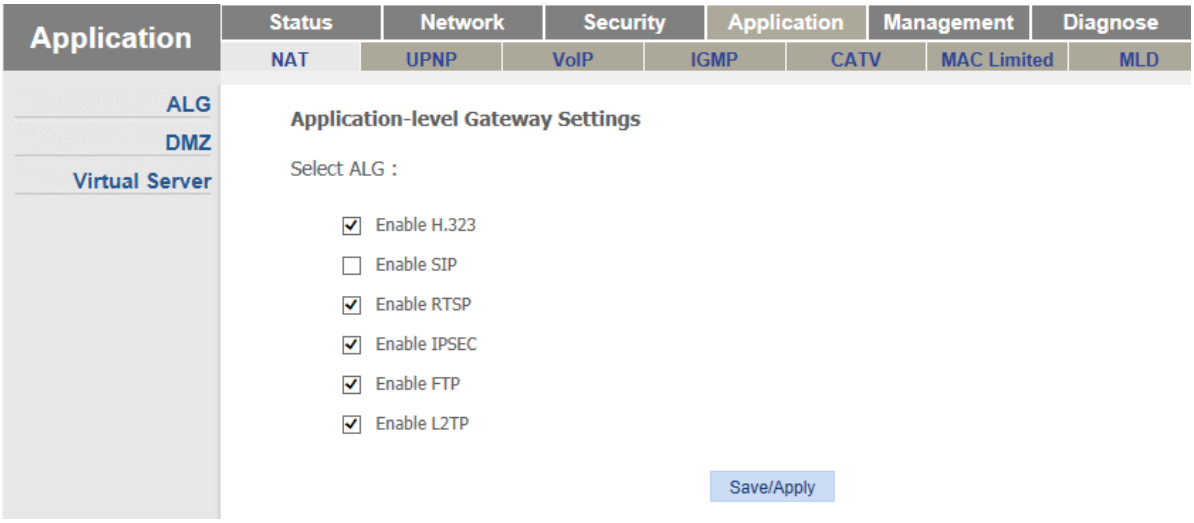
UPnP (Universal Plug and Play) ist eine Zusammenarbeit von Protokollen, durch welche die Verbindung von Geräten möglich wird. Damit können Sie konfigurationsfrei über ihr Netzwerk miteinander kommunizieren. Media-Streaming ist der am häufigsten genutzte Dienst, da dadurch Mediendateien (Filme, Musik, usw.) direkt zu Ihrem TV-Gerät, Tablet oder Smartphone gestreamt werden können. Voraussetzung dafür sind die entsprechenden Apps auf Ihren Geräten!

Nach der Aktivierung klicken Sie auf "**Save/Apply**", um die Einstellung dauerhaft zu speichern.

NAT ALG Settings

Im Webinterface Ihres Routers, klicken Sie auf "**Application**" in der obersten Reihe, dann auf "**NAT**" und schließlich auf "**ALG**" auf der linken Seite.

Die NAT Application-Level Gateway Einstellungen erscheinen.



Hier können Sie folgende Einstellungen vornehmen:

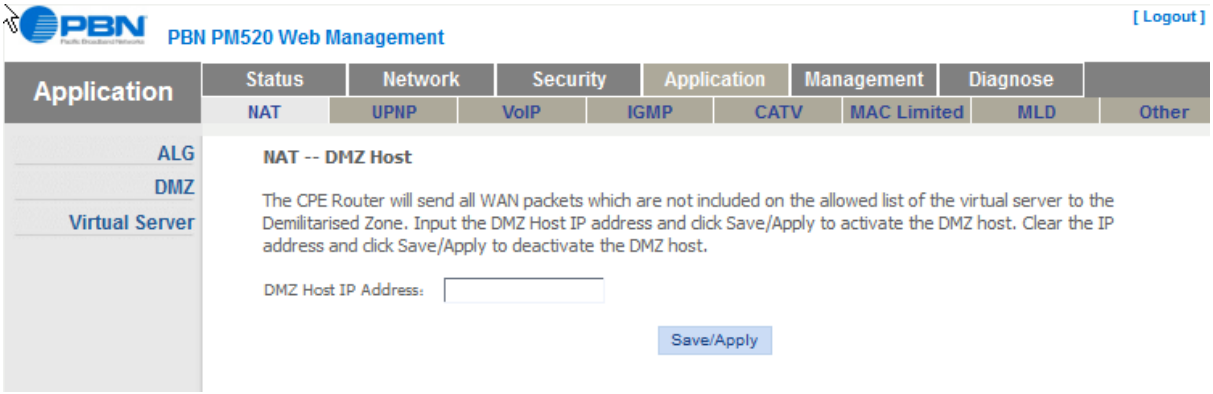
- aktivieren/deaktivieren H.323 Access
- aktivieren/deaktivieren SIP
- aktivieren/deaktivieren RTSP
- aktivieren/deaktivieren IPSEC
- aktivieren/deaktivieren FTP
- aktivieren/deaktivieren L2TP
- aktivieren/deaktivieren

Klicken Sie nach dem Ändern auf **"Save/Apply"**, um Ihre Einstellungen dauerhaft zu speichern.

NAT DMZ Settings

Im Webinterface Ihres Routers, klicken Sie auf "**Application**" in der obersten Reihe, dann auf "**NAT**" und schließlich "**DMZ**" auf der linken Seite.

Die NAT DMZ Einstellungen erscheinen.



Hier können Sie einen lokalen Computer oder eine IP-Adresse (Host) als DMZ (Demilitarized Zone) konfigurieren.

Ein DMZ Host wird nicht durch die Firewall geschützt und ist somit leicht angreifbar. Wenn Sie einen DMZ Host konfigurieren, müssen Sie das Sicherheitsrisiko berücksichtigen und sich gegebenenfalls selbst vor Attacken schützen.

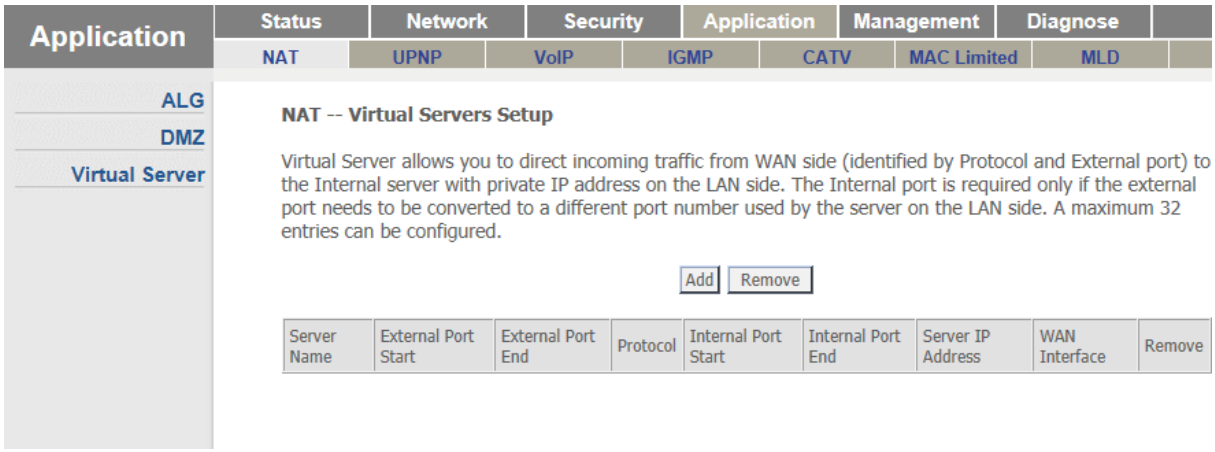
Wollen Sie nur einzelne Ports für das Internet öffnen, so verwenden Sie bitte die Funktion **Virtual Server (Port Forwarding)**

Klicken Sie nach dem Ändern auf "**Save/Apply",** um Ihre Einstellungen dauerhaft zu speichern.

NAT Virtual Server Settings

Im Webinterface Ihres Routers, klicken Sie auf "**Application**" in der obersten Reihe, dann auf "**NAT**" und schließlich "**Virtual Server**" auf der linken Seite.

Die NAT Virtual Server Einstellungen erscheinen.



Klicken Sie auf "**Add**" um zum Konfigurationsschirm zu gelangen. Hier können Sie vorkonfigurierte Einstellungen wählen oder eigene Port-Forwards einrichten. Verwenden Sie dazu immer das Interface „43_INTERNET_R_VID_401/epon0.3".

Wenn Sie eine Regel hinzugefügt haben, klicken Sie auf „**Apply/Save**" um diese zu speichern. Um eine Regel wieder zu entfernen, wählen Sie diese über die Checkbox aus und klicken Sie auf "**Remove**".